The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED: November 2, 2012

SUBJECT: Possible spear phishing campaign to start on or after November 1, 2012

BACKGROUND

The MS-ISAC received a report from a trusted third party related to a spear phishing campaign that may be targeting State, Local, Tribal, and Territorial governments.

Spear phishing is an e-mail spoofing fraud attempt that targets a specific sector or organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

This particular spear phishing campaign may be originating from “GhostNet”, a large-scale cyber-spying operation based mainly in the People’s Republic of China. If executed, the malicious files contained in the spear phishing e-mail will execute a version of the “Gh0st Rat” Trojan, the “Rat” portion of the name referring to the Trojan’s ability to act as a “Remote Administration Tool”.

DETAILS

The reported spear phishing attack appears to be originating from *webmaster@<U.S. State-level Department>.gov*, and includes the malicious attachment “Details.xls”. When executed, the attachment drops and opens another file named “Details.xls” as well as an executable file named “rspcap.exe”.

1. The second “Details.xls” is a benign Excel document that is displayed to the user, intended to distract attention from the malicious executables, and the document may contain the following content:

    Claiming to be: Chaise.Auten@yahoo.com
    Content type: Virus
    Our internal reference code for your message: 24298-04/qMKlnxtbYuCv
    First upstream SMTP client IP address: 69.188.235.22
    According to a ‘Received: “ trace, the message apparently originated at: 69.188.235.22
    Return-Path: Chaise.Auten@yahoo.com
    From: playboy playboy@yahoo.com
    Message-ID: 201210310947.q7E9lA1v025618@yahoo.com
    Subject: Congratulations!

2. “rspcap.exe” drops and executes the following files: “rspcap.exe.bat”, “read.exe”, “Acrofx32.exe”, and “daemon.exe”.
3. “rspcap.exe.bat” deletes "rspcap.exe", then itself.
4. “read.exe” creates the following registry key for persistence (i.e. setting the Trojan to run at boot):

   HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Messenger = C:\Documents and Settings\<User>\Application Data\Microsoft\MSN\Acrofx32.exe

5. “Acrofx32.exe” deletes “read.exe” and executes “daemon.exe”.
6. “daemon.exe” is the backdoor Trojan known as “Gh0st Rat”. It sends a DNS query for “gov.communityapan.com”, then sends traffic to the resolved domain, over port 443/tcp, with packets beginning with the string Adobe, searching for additional instructions and/or downloads. The following is an example trace:

   00000000 41 64 6f 62 65 a9 00 00 00 e0 00 00 00 78 9c 4b Adobe… …..x.K
   00000010 63 62 62 98 c3 c0 c0 c0 0a c4 8c 40 ac c1 c5 c0 cbb….. …@....
   00000020 c0 04 a4 83 53 8b ca 32 93 53 15 02 12 93 b3 15 ….S..2 .S……
   00000030 8c 19 6a 4e e8 4e ac 91 00 8a 77 c4 09 83 71 c2 ..jN.N.. ..w…q.
   00000040 a5 09 35 0c 60 c0 c8 e0 13 2f cc 10 53 d3 5c 03 ..5.’… ./..S.\.
   00000050 12 07 01 51 a0 58 0a 90 2f c2 60 00 36 eb 07 d0 …Q.X.. /.’.6…
   00000060 70 1d 16 06 38 38 73 6b 02 dc bc 1b 40 3d 37 d0 p…88sk ….@=7
   00000070 cc 9b 03 34 8f 19 cc 64 64 d8 c0 0d a2 18 99 4a …4…d d……J
   00000080 8b 53 8b 0c a1 fa 77 78 22 cc d2 a8 11 65 88 00 .S….wx “….e..
   00000090 aa b7 f9 36 a1 c6 11 88 41 fc 02 20 9f e1 03 03 …6…. A.. ….
   000000A0 83 1d 50 1e 00 88 cd 2a ef ..P….*

The file details are as follows:

Details.xls (attached file)
MD5: 154b993c89a7ed244f70e95c6a444919
Size: 159255 bytes

Rspcap.exe
MD5:153739d197c78f35dfe1482e4bd60
Size: 111104 bytes

Details.xls (dropped file)
MD5: a525734600aa1e5743e50dcef0854e09
Bytes:20992 bytes

rspcap.exe.bat (This is a dynamically generated script, so size and MD5 may vary between installations.)
MD5: abc9551a06c35ea0ccd61b9bc509734c
Size: 113 bytes

Read.exe
MD5:b867be0e9b32fd044abc3ae1b99ff380
Size: 2560 bytes

Acrofx32.exe

MD5: bb0c81d943c570d6d6b719fbe69b3322
Size: 3584 bytes

Daemon.exe
MD5: 642505ec7274255894716c2fcf22eab0
Size 98816 bytes

Domain Details:
communityapan.com

RECOMMENDATIONS:
The following actions should be taken:
Check the network logs for identifying traffic to the aforementioned domain.
Ensure that all systems are running up to date antivirus and have updated signatures.
Remind users not to open email attachments or click on URLs from unknown or untrusted sources.
Review the email logs for receipt of any email from webmaster@<U.S. State-level Department>.gov
Implement email policies to flag all incoming email from webmaster@<U.S. State-level Department>.gov, or with the attachment "details.xls" at your email gateway.
Block all traffic to the IP addresses and domain identified above and log any connection attempts
Apply all vendor patches after appropriate testing.

If you believe you are experiencing a Spear Phishing attack, please notify MS-ISAC by sending an email to soc@msisac.org.

REFERENCES:

Center for Internet Security
http://www.cybergriffin.com/cyber-safety-tips/documents/CGSpearPhishingtipssheet.pdf

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov/reading_room/phishing_trends0511.pdf

F-Secure
http://www.f-secure.com/weblog/archives/ghostnet.pdf

Anti-Phishing Working Group (APWG)
http://www.antiphishing.org